A Novel Learning based Secured Data Evaluation Scheme using Cybersecurity Principles with Artificial Intelligence Logic

S. KAMATCHI[1], C.SRINIVASA RAJU[2], R. M.DILIP CHARAAN[3], E. SIVAJOTHI[4],
SUJATHA JAMUNA ANAND[5], N. S. GOWRI GANESH[6]
[1]Department of Electronics and Communication Engineering,
Saveetha School of Engineering,
Chennai,
INDIA

[2]Department of Humanities,
Madanapalle Institute of Technology & Sciences,
Andhra Pradesh,
INDIA

[3]Department of Computer Science and Engineering,
Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology,
Chennai,
INDIA

[4]Department of Computer science and Engineering,
Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology,
Chennai,
INDIA

[5]Department of Electronics and Communication Engineering,
Loyola Institute of Technology,
Chennai,
INDIA

[6]Department of Artificial Intelligence and DataScience.
Saveetha Engineering College,
Chennai,
INDIA

Abstract: - Due to the Internet of Things and the digitalization revolution, there is nowadays an overwhelming amount of cybersecurity information in the tech world. Dealing efficiently with cyber deviations and attacks is an emerging challenge to any cyber security industry all over the world. Traditional security solutions can no longer address today's security threats because of the rapid proliferation of various cyber-attacks and threats. Artificial intelligence understanding, especially machine learning technology can make a security system up to date by analyzing its security data so that the safety mechanism can be upgraded continuously and so that it can remain programmatic and automated. This study provides a comprehensive overview of existing machine-learning techniques inspired by the notion of AI. We explore its capabilities of advanced information analytics and management by deriving meaningful conclusions out of cyber data in Cybersecurity. The performance of the proposed method will be compared against that of a standard machine learning technique, Support Vector Machine (SVM), using cross-validation. This scheme is known as a Secured Learning based Data Evaluation Scheme (SLDES). Based on its analysis of past incidents and knowledge summaries from experts, the proposed AI approach SLDES (Shift Left Diverse Experiments and Simulations) would change or reform newly appearing sections as it retrieves recent events. Last but not least we present our research about the future of artificial intelligence in information security etc. Machine learning and its related approaches are being investigated and used in cyber defense, and the focus of the described section is to evaluate the current and

future uses of machine learning in cyber defense, for the scheme proposed the section presented the way to demonstrate how to effect the proposed scheme is and the result metrics are plotted in histogram form To derive such insights and information necessary for designing countermeasures for such attacks, even as stated in, a thorough data analysis is important. The main aim of this research is to establish that clients can develop a safe situation to protect their electronic data from intruders.

Key-Words: - Novel Learning, Data Security, Data Evaluation, Cybersecurity, Artificial Intelligence, AI, SLDES, Machine Learning, Support Vector Machine, SVM.

Received: July 16, 2024. Revised: March 19, 2025. Accepted: April 15, 2025. Published: May 21, 2025.

1 Introduction

In our interconnected digital world in 2020, there are various types of technology, company cultures, and processes, [1]. This allows cybercriminals to move around opportunistically within the workplace, which acts in their favor. (Expect to meet a constant stream of invaders and attackers regardless of the organization). With an eye on both large and small entities, they are seeking to disrupt the public and private sectors alike. Thus, defensive tools, techniques, and algorithms of cyber-security have to uncover the identities of cyber attackers and destructive scenarios, [2]. A cyber security system is one that uses a variety of algorithms and techniques to do so to sabotage, attack, or access unwanted data, networks, and nodes, [3]. Large organizations consist of bytes of data (this data includes the organization's highly sensitive information and critical information) [4] and due to this reason, it is one of the most popular motives of those organizations to save their data from being accessed by unauthorized parties and threats which could really harm the organization, to protect an organization, the cyber defense is used to defend common attacks (manipulation of existing vulnerability), advanced assaults (involves exploiting complicated flaws) and used against new buttons, [5]. The information system structures itself among a number of diverse departments of the organization such as the production, operations, and management departments, [6].

In today's era, computers are everywhere and nearly everything we use today is connected to the Internet in an ecosystem called the Internet of Things, [7]. These devices talk to one another, and transmit their data across the Internet, which is a communication medium full of security holes. This is sensitive material the vast majority of the time. It's always the harmful entities like these online attackers looking for that, where they can play with the things (they can go with many attacks like replay attack, man-in-middle attack, impersonate, guess the credentials, compute the session-specific key, inject malware (data can't be altered simply while you play with the things) and alter the data while playing the thing). Therefore, in the interest of defending against such attacks, several researchers may occasionally propose their own new security systems, [8]. These security protocols which are also referred to as cyber security protocols can be grouped into various types of protocols such as authentication protocols, access control protocols, intrusion detection protocols, key management protocols, blockchain-enabled security protocols, [9], [10].

(i) Protocols for Authentication: Authentication is the process of confirming the user or device identity. This can use elements or credentials directly related to the person or device (for example biometrics, smartcard, username, and password), [11]. Users can authenticate with users, devices can authenticate with devices, devices can authenticate with users, or users can authenticate with devices.

(ii) Protocols for Controlling Access: Access control is a way of preventing unauthorized people or devices from accessing a system. Once users or devices have gone through every step of an access control protocol, they can communicate securely with one another. Access control protocols can be broadly classified into two categories — User access controlled protocols and Device controlled access protocols. User access control protocol is used to control unauthorized users, and device access control protocol is used to control unauthorized devices.

(iii) Protocols for Detecting Intrusions by Malevolent Actors: Anything that enters without permission is an intrusion. The consequence can be a system of control by the hacker or a harmful programming script. Hackers often inject malware into internet devices to disrupt their security or performance.

(iv) Protocols for Key Management: Protocols are in place for secure key management among some entities, for instance, smart vehicles and

Internet of Things (IoT) devices, and also among certain individuals, such as smart home users, physicians, and traffic inspectors, and so on.

(v) Modern Security Procedures that make use of Blockchain Technology: Blockchain is a different type of technology. In a blockchain, data is stored in blocks that are cryptographically linked by their hash value. Blockchain refers to the distributed ledger technology in which blockchain data is stored, and blockchain technology, [12].

Cybercriminals will continue to become more advanced in their ability to hide from detection; for example, several of the latest malware kits have included techniques for avoiding antivirus and other threat detection technologies. But Cybersecurity has arrived at a vital juncture, where instead of depending on defense and mitigation, future science and research should devote their attention and efforts to predict systems addressing cyber-attack prediction systems to foresee significant events and their influence. Systems should be organized around broad, predictive studies of cyber risks, globally. Cybersecurity needs to predict, prevent, identify, and detect automated and intelligent, [13], [14].

The technique called Denial of Service (DoS) if it's from a single device, or Distributed Denial of Service (DDoS) if it's from multiple machines, an attack seeks to make a service, network, or server unable to handle any more connections due to an excess of Internet traffic. Distributed denial of service attacks use a network of exploited machines to bombard a given victim with floods of spam, [15]. These infections may be caused by a botnet: a network of infected computers manipulated by a single nefarious actor. This led to two reasons the Distributed Denial Of service attacks are popular and dangerous in the current networks. First of all, several types of normal DoS attacks have already been mitigated by new safety gear. And DDoS attack appliances are now both inexpensive and easy to deploy, [16].

Cyber security focuses on defending systems and data against malicious cyber attacks. Cyber threats can manifest in multiple ways, including viruses, malware, data mining, and application breakouts. The need for an automated threat evaluator has increased within an organization or company over the past few years due to the increased number of cyber-security attacks, [17]. Cybersecurity is essential for multiple enterprises because the devices involved in data are everywhere and can be utilized as point-of-access for criminals. The cyberattacks seem to be more global and organized, so the government decided to devote more resources to exploring means to curb different cyber threats. Figure 1 depicts cyber security-related fields, [18].

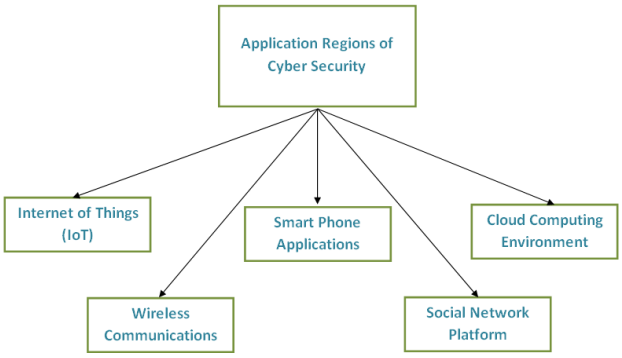

Fig. 1: Fields Related to Cybersecurity

2 Related Study

Deep Learning [19], [20] has been successfully used to detect various types of network attacks. But there have not yet been any examples out in the wild, in a case that is not purely a lab setting, of scenarios in network security that show how deep learning algorithms can be applied. And, due to the techniques being used, high-performance computing-building systems are needed to handle the colossal amounts of traffic. In light of the dynamic nature of cyberattacks, we designed and implemented our AIIDS (AI-based Intrusion Detection System). We present a simple but effective CNNLSTM-based architecture that combines convolutional neural networks with long short-term storage networks for obtaining accurate features from real-time HTTP plaintext data without the need for calculating entropy or compression. The model is normalized UTF-8 character-based and is for Spatial Feature Learning (SFL) specific.

To prove it, we retried this process several times using two openly available datasets (CSIC-2010, CICIDS2017) and non-variable real-time data. To enable the AI-IDS to classify malicious vs non-malicious data, it trains payloads and a labeling tool to research true/false positives. It has only this way to interpret multi-faceted attacks with unknown structures, coded or slimed attacks, etc. This is based on Docker images, which allows you to separate user defined functions into different images. It is also flexible and scalable. This is also helpful in composing and hone Snort rules for signature-based intrusion detection systems when new patterns are discovered. The model can accurately analyze unknown web-attacks by

continuously training and it calculates all the harmful probability, [21].

The task of achieving cyber-security has been gradually increasing in recent times due to the terrifying trend in the range of functions linked to computers and the connectivity of such gadgets, [22]. It also demands a solid defense system to resist a wave of cyberattacks. It is, therefore, important for cyber-security to construct an intrusion detection system (IDS) capable of detecting network attacks and anomalies. We have developed a data-driven intrusion detection system that does a good job of utilizing AI, in particular, machine learning tools. This paper presents a method for identifying breaches generated through Intelligent services in the cyber-security domain by employing a set of popular machine learning classification algorithms such as Bayesian Network, Naive Bayes classifier, Decision Tree, Random Decision Forest, Decision Table, and Artificial Neural Network. Finally, we evaluate the performance of various experiments on cyber-security data that include numerous cyber-attack types. We analyze motivation metrics such as accuracy, f1-score, recall, and precision, [23].

For example, when hackers use malicious data injection attacks (MDIAs), they change the readings of the SCADA system and WAMS systems, which greatly reduces the cyber-physical power system's (CPPS) capacity to estimate the current status, [24]. Even though MDIA can spread across the communication network of CPPS as a type of network attack and have a significant effect on the secure functioning of CPPS, the majority of existing research ignores PMU vulnerabilities in WAMS and focuses on SCADA systems. Therefore, to address these challenges, we propose a SCADA and WAMS-based hybrid measurement network scheme to minimize the risks. The initial stage involves the suggestion with the state predictor and so the harmful data identifier together supplying a system regarding the identification associated with the hazardous data depending on the dynamic temporal warping (DTW) distance, [25]. It proceeds to provide a risk mitigation model, which based on the results of attack detection disables the compromised meters that were caused by the diffusion of malicious data. This method greatly reduces the risk level of the system, maintaining the observability of the CPPS. Finally, we present a way for hybrid measurement networks to work in concert to observe MDIAs and apply them to the risk mitigation strategy in multiple scenarios, [26].

For the power sector, the adoption of cyber-physical power systems (CPPS) is accelerating. These CPPS contain millions of sensors to generate terabytes of data. Basically, as we have data from all these sensors, not only can we make our CPPS more efficient and reliable, but we can also expand the danger landscape. Fake data injection attacks (FDIAs) are one attack vector that has greatly affected the energy management practices involving CPPS. Existing data-driven approaches to FDIA design assume different factors and have external dependencies that can make them impractical or, most importantly, vulnerable bad data detection (BDD) algorithms. In this work, we review previously proposed data-driven FDIA designed to be evaluated with varying types of measurement data. In addition, we propose an RLR-based data-driven attack method. If enough measurement data is considered, evaluation case studies are formed for every data-driven assault. Our proposed RLR strategy significantly outperforms competing data-driven approaches [27], even in the presence of extreme cases.

One of the cyber-physical threats in ISMGs that urgently requires attention is a false data injection attack (FDIA), which falls within the category of typical accretion attacks. This work [28] proposes a new method for detecting cyber-attacks, in particular FDIAs based on the fast Fourier transform (FFT) and singular value decomposition (SVD). As most of the recent works focused on accommodating such malicious attacks in DC systems, it should be noted that similar attacks can also be considered for AC systems. As a result, in SI analysis and in the consideration of the impact of renewable energy sources, AC state estimate (SE) has been used. If abnormal data is added to state vectors, the relations concerning the temporal and spatial datum of the vectors become different than they are found during normal operation, [29]. A switching surface—similar to that which would be dialyzed by a sliding mode controller to control the accurate sets of FFT coefficients—was used to determine the singular values that were evaluated. To detect cyber-attacks, FFT and SVD composition are applied to obtain the indexes of the voltage/current switching surface. The Agent such as smart sensors, control units, smart loads, and others, role of them is to interchange the signal and their protective scheme is proposed to detect cyber-attacks. The same is seen in the various techniques employed for FDIA, like amplitude and vector decomposition of signals. Particularly, in multiple case-study types, the proposed detection scheme significantly lowers the time (i.e., less than ten milliseconds from the beginning of the assault), which represents the main beneficial feature. The

detection accuracy for the proposed method is greater than 96% on 2967 tests, [30].

3 Methodology

Every network security system should have some effective, strong as well as scalable malware detection capabilities. Cyber-attacks were rare in the early Internet. Data gathered by the antivirus's malware detection modules about an item is used to determine whether it is dangerous. Data on data, Data on data, One potential source of data on data comes from the time before the file is run: Because of the widespread adoption of the Internet and the ever-growing complexity of malware, manual detection criteria are no longer adequate and new enhanced security mechanisms are needed. During the detection and classification of malware, malware writing relies on machine learning, which is a subset of artificial intelligence that helps to carry out functions such as detection, file search and recognition, and even making decisions.

Machine learning is better than humans at pattern recognition and prediction. In elaborate, dynamic network systems, security perception and policy tuning have not met expectations. Advanced automation of intelligent decision-making is now possible due to progress in machine learning. So, protecting an information system, especially one connected to the Internet, against various kinds of cyber threats, attacks, destruction or unlawful access is a serious and crucial issue that needs to be addressed immediately. This study proposes a novel Secured Learning model-based Data Evaluation Scheme (SLDES) that is more efficient in analyzing and sharing threat data and information than the existing approach, Support Vector Machine (SVM). Figure 2 displays a range of typical cyber-attacks or threats.

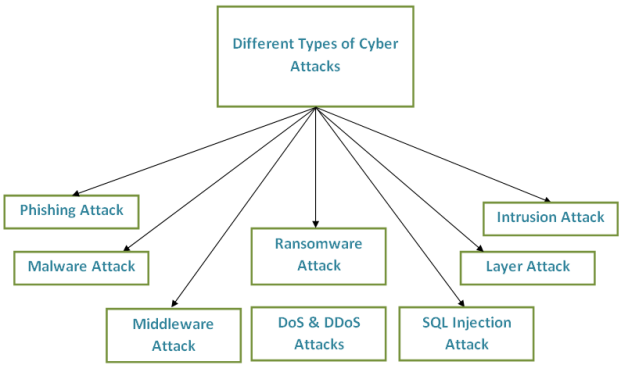

Fig. 2: Assortment of Typical Cyber Attacks or Threats

Third-party attacks, which can take many forms in computer networks

(i) Eavesdropping: Eavesdropping, alternatively known as a sniffing or snooping assault, typically refers to a passive form of cyber, or network, attack. In this type of attack, an enemy is trying to eavesdrop on the parties' private communication.

(ii) Replay Attack: A retransmits the previous exchanges that it has recorded on purpose.

(iii) Analyzing Traffic: The second kind of JoINS attack is a non-active attack. In this kind of attack, an adversary A eavesdrops on an existing conversation, and uses what it hears to gain information about the subject of the conversation, the attitude of the speaker, the trajectory of the conversation, the time and place of the eavesdrop, and more. Using the data obtained, A is now able to conduct various other reconnaissance attacks.

(iv) Man-in-the-Middle Attack: In a man-in-the-middle attack, the assailant contacts two separate communication entities, passing the communication between them. In this scenario, both sides involved in the discussion believe they are communicating with one another.

(v) Impersonation Attack: An impersonation attack is an active class of attack in which an adversary takes on the identity of a legitimate party on the network and sends altered or new messages to another legitimate party on the network.

(vi) Denial-of-Service (DoS) Attack: A Denial-of-Service (DoS) attack is where A inundates the victim's computer resources with a large number of false requests. This makes it impossible for us to fulfill the request of the legitimate user for service.

(vii) Malware Attack: The use of the victim computer to run the harmful script. When received or installed, malware is a program (or in some instances file) that will hack, encrypt illegally stored data, change data, or erase data from computers.

Figure 3 distinguishes the stages of machine learning-based prediction model training and testing.

The explosive growth of data technology is causing so many to increasingly rely on the ties of the community to engage in secure commercial dealings. Indeed, the increased cyberattacks threaten both networks and communications. Implementing security measures is salient to mitigate unauthorized alteration, corruption, and dissemination of sizeable information as conducted on sensitive human, government, and military networks. Word filters IP blacklists, message filtering, and even sender reputation mapping—the old go-to techniques for fighting spam and phishing—no longer cut it. With heterogeneous systems producing many different

types of raw data formats, the cyber security profession must tackle a variety of challenges. However, raw data on such functions may be effectively utilized by machine learning due to its capabilities.

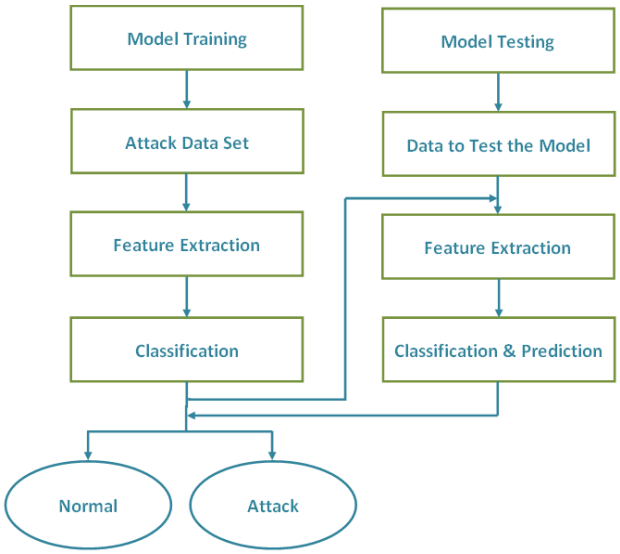

Fig. 3: Stages of a Prediction Model that is based on Machine Learning and is being Trained and Tested

4 Results and Discussions

Any of these security vulnerabilities can be exploited, and any attack would qualify as an assault. Cybersecurity can be defined as the actions taken to prevent and detect cyberattacks, particularly the most damaging types, such as phishing and malware. But a close cousin of this type of social engineering called "phishing," where the perpetrator impersonates a business or organization, is a widespread form of "brand cloning," with the goal of stealing sensitive information. Support Vector Machines (SVM) is the most widely applied and successful machine learning implementation for intrusion detection schemes and an appropriate alternative is proposed by the Secured Learning based Data Evaluation Scheme (SLDES). The separation and classification of the two data classes are performed by the SLDES and SVM toward labeling the margin on either side of the hyperplane. When it comes to classification, the greater the distance from hyperplanes and margins, the more favorable the outcomes. There are data points on the edge of the hyperplane called support vectors. The proposed SLDES and SVM algorithms for machine learning are classification methods. This binary classification technique finds the optimal n-dimensional hyperplane from a training set. Data are classified in the two-dimensional surfaces and multifunctional hyperplanes applying the SLDES and SVM algorithms. A multidimensional hyperplane works with a kernel approach to be able to classify data in a multidimensional way. Having as much separation in classified data sets is preferred. In other words, the maximum margins or distance between the data points must be used for the hyperplanes. A hyperplane is a border separating two planes.

SLDSE and SVM algorithms are used to classify multidimensional data, where a hyperplane is a dual-dimensional plane with three or more inputs. The primary use case of SLDES and SVM Algorithms is for classification whereas regression analysis is another possible use. A classification algorithm examines the data inspected for training to predict what will occur. The final product is a class, such as Day, Night, Yes or No, or Long or Short. For example, a customer who buys bread and butter at the same time from a store could be an example of one class. The intended audience would respond with a yes or no. Regression analysis, which acts as a forecasting tool for results is used to identify the relationship of independent variables. SLDES and SVM are two different groups. So the kernel function defines the space, it can be linear or non-linear. The degree of its recognition will dictate if this is one category or several. To train SLDES with various time intervals and obtain better learning for flexible consumption structures, the kernel functions with appropriate parameters have been utilized. Because SLDES and SVM are both memory-intensive and time-consuming,

The validation accuracy for the proposed method, Secured Learning Data Evaluation Scheme (SLDES) is shown in Figure 4 along with the standard model (SVM) to check the effectiveness of the developed method against training accuracy. The same information is presented below in a tabular form Table 1.

Table 1. Training Accuracy

S.No.	Epochs	SVM (%)	SLDES (%)
1.	100	83.64	94.68
2.	125	83.26	94.82
3.	150	83.51	94.77
4.	175	83.48	94.85
5.	200	83.29	94.76
6.	225	83.29	94.83
7.	250	83.24	94.85
8.	275	83.20	94.87
9.	300	83.15	94.89

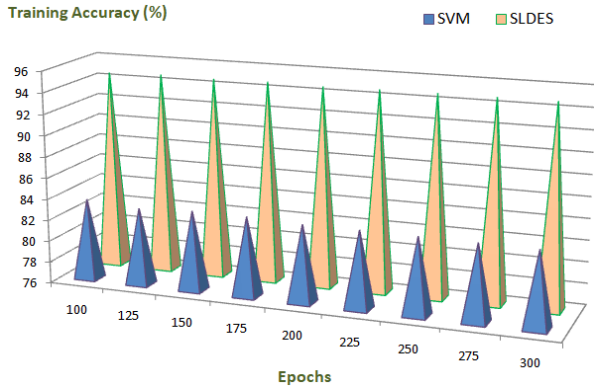

Fig. 4: Training Accuracy

In order to assess the testing accuracy of the suggested scheme, SLDES is cross-validated with the traditional model SVM, as shown in the accompanying Figure 5. You may find a more detailed description of the same in Table 2.

Table 2. Testing Accuracy

S.No.	Epochs	SVM (%)	SLDES (%)
1.	100	86.31	96.38
2.	125	86.29	96.41
3.	150	86.42	96.39
4.	175	86.37	96.18
5.	200	86.43	96.37
6.	225	86.46	96.28
7.	250	86.49	96.37
8.	275	86.52	96.52
9.	300	86.55	96.51

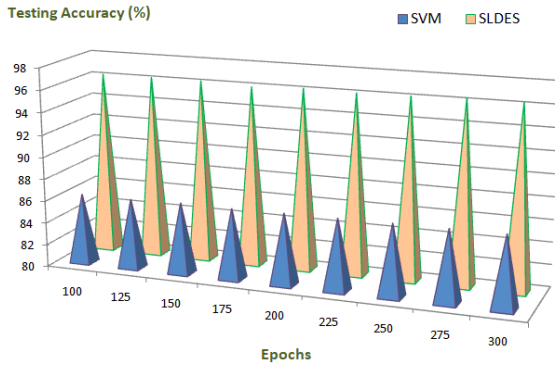

Fig. 5: Testing Accuracy

As shown in Figure 6, the training loss ratio of the suggested method, SLDES, is compared to that of the more traditional model, SVM, in order to assess the efficacy of the latter. What follows is a descriptive table of the same information, Table 3.

Table 3. Training Loss

S.No.	Epochs	SVM (%)	SLDES (%)
1.	100	2.65	0.85
2.	125	2.71	0.96
3.	150	2.34	0.98
4.	175	2.47	1.01
5.	200	2.51	1.09
6.	225	2.38	1.14
7.	250	2.56	1.19
8.	275	2.64	1.24
9.	300	2.69	1.30

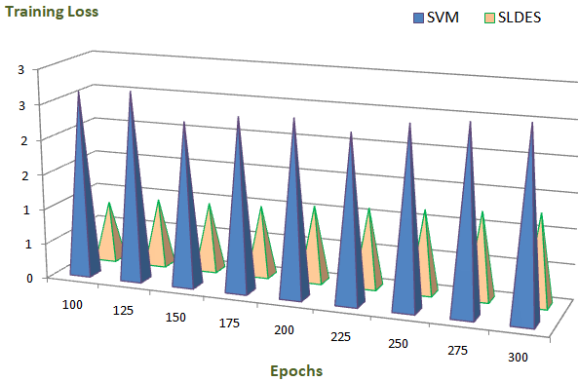

Fig. 6: Training Loss

In order to assess the testing loss ratio of the suggested method, SLDES, it is cross-validated with the traditional model, SVM, as shown in Figure 7 underneath. You may find a more detailed description of the same in Table 4.

Table 4. Testing Loss

S.No.	Epochs	SVM (%)	SLDES (%)
1.	100	3.26	1.09
2.	125	3.29	1.14
3.	150	3.41	1.17
4.	175	3.47	1.19
5.	200	3.52	1.23
6.	225	3.60	1.26
7.	250	3.67	1.30
8.	275	3.74	1.33
9.	300	3.81	1.36

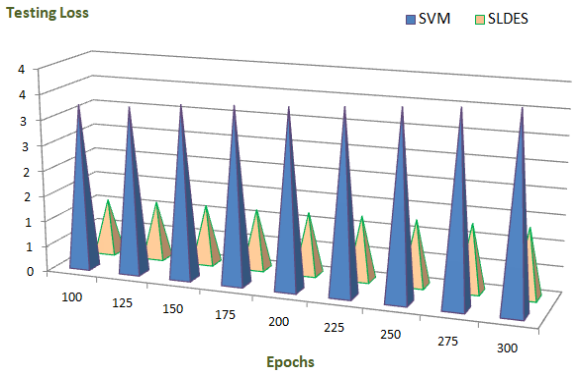

Fig. 7: Testing Loss

In order to assess the accuracy ratio of the suggested method, SLDES, it is cross-validated with the traditional model, SVM, as shown in Figure 8 which follows. You may find a more detailed description of the same in Table 5.

Table 5. Precision

S.No.	Epochs	SVM (%)	SLDES (%)
1.	100	78.14	95.34
2.	125	78.21	95.19
3.	150	78.17	95.27
4.	175	78.26	95.36
5.	200	78.64	95.39
6.	225	78.60	95.39
7.	250	78.70	95.42
8.	275	78.81	95.45
9.	300	78.91	95.47

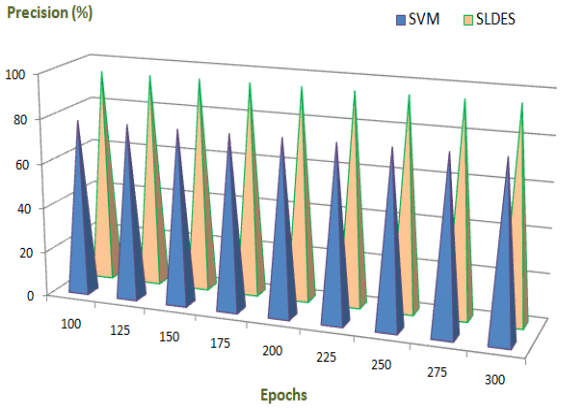

Fig. 8: Precision

In order to assess the recall ratio of the suggested method, SLDES, it is cross-validated with the traditional model, SVM, as shown in Figure 9 which follows. Further, a more detailed description of the same is presented in Table 6.

Table 6. Recall

S.No.	Epochs	SVM (%)	SLDES (%)
1.	100	52.64	76.31
2.	125	52.82	76.27
3.	150	52.71	76.39
4.	175	52.68	76.54
5.	200	52.73	76.51
6.	225	52.73	76.38
7.	250	52.73	76.81
8.	275	52.74	76.72
9.	300	52.74	76.79

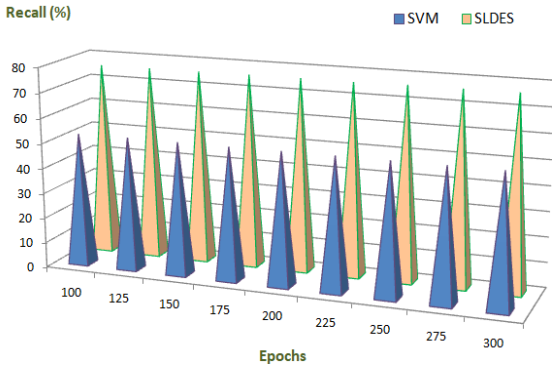

Fig. 9: Recall

In order to assess the F1-Score ratio of the suggested method, SLDES, it is cross-validated with the traditional model, SVM, as shown in Figure 10 which follows. Further, a more detailed description of the same is presented in Table 7.

Table 7. F1-Score

S.No.	Epochs	SVM (%)	SLDES (%)
1.	100	56.39	79.36
2.	125	57.21	79.95
3.	150	57.58	80.09
4.	175	57.94	80.53
5.	200	58.54	80.90
6.	225	59.04	81.26
7.	250	59.54	81.63
8.	275	60.04	81.99
9.	300	60.54	82.36

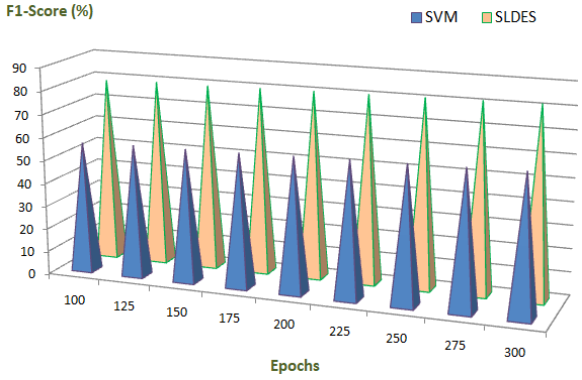

Fig. 10: F1-Score

In order to assess the Sensitivity ratio of the suggested method, SLDES, it is cross-validated with the traditional model, SVM, as shown in Figure 11 which follows. Further, a more detailed description of the same is presented in Table 8.

Table 8. Sensitivity

S.No.	Epochs	SVM (%)	SLDES (%)
1.	100	74.36	87.56
2.	125	74.29	87.49
3.	150	74.37	87.52
4.	175	74.41	87.64
5.	200	74.42	87.62
6.	225	74.44	87.65
7.	250	74.46	87.67
8.	275	74.48	87.70
9.	300	74.51	87.73

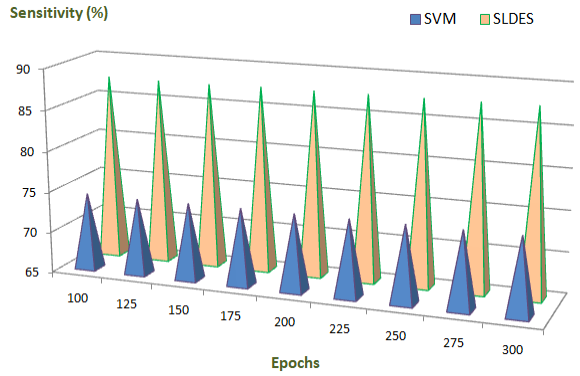

Fig. 11: Sensitivity

In order to assess the Specificity ratio of the suggested method, SLDES, it is cross-validated with the traditional model, SVM, as shown in Figure 12 which follows. Further, a more detailed description of the same is presented in Table 9.

Table 9. Specificity

S.No.	Epochs	SVM (%)	SLDES (%)
1.	100	81.26	89.34
2.	125	81.34	89.47
3.	150	81.39	89.62
4.	175	81.42	89.76
5.	200	81.49	89.90
6.	225	81.54	90.04
7.	250	81.59	90.18
8.	275	81.64	90.32
9.	300	81.70	90.46

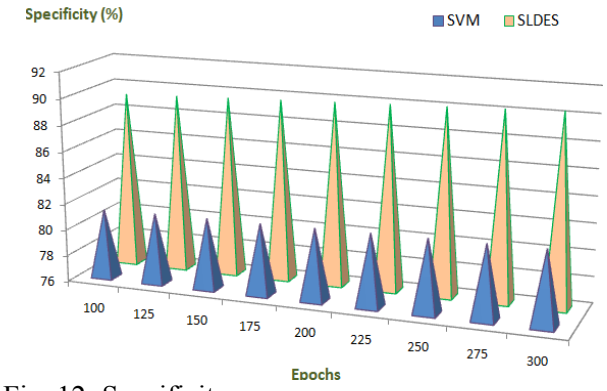

Fig. 12: Specificity

5 Conclusion

The results of the study indicate that perimeter-based, historical data-driven cyber defenses are prevalent today. Thus, it is harder to discover new cyber threats leveraging these methods. Using a mix of multiple threat sensors and deeply baked-in tactics, it is entirely possible to defend against attacker campaigns that succeed and also to contain follow-on attacks. Entities can exchange risk patterns through threat information sharing, which can be used for threat analysis and responding to occurrences. One significant issue is that they do not cover all the relevant information and facts needed to allow for effective threat intelligence. To encourage higher-level thinking, knowledge must be extracted and described from publicly available data. Although data mining methods seem promising for detecting such dangers, training a model or, even an artificial neural net to avoid this type of unexpected dangers still requires human understanding. The research also concluded threat intelligence relies on the efficient assessment and sharing of threat Information and data. All will gain when everyone is singing from the same hymn sheet on the protocol, format, representation, language, etc. So AI solution is the best choice for solving this problem. Part of that assessment involves using statistical tools to assess threat intelligence from data mining. It also has the potential to work with data mining and artificial intelligence systems to identify previously nonexistent patterns of threats, which would only further extend the reach of the paper.

References:

[1] T.Soeewu, et al., *"Analysis of Data Mining-Based Approach for Intrusion Detection System"*, IC3I-22, 2022. https://doi.org/10.1109/IC3I56241.2022.10072828.

[2] Y. Shin and K. Kim, "Comparison of anomaly detection accuracy of host-based intrusion detection systems based on different machine learning algorithms", *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 2, pp. 252-259, 2020. doi: 10.54216/JCIM.140102.

[3] H. A. Hassan, E. E. Hemdan, W. El-Shafai, M. Shokair and F. E. A. El-Samie, "Intrusion detection systems for the Internet of Thing: A survey study", *Wireless Pers. Commun.*, vol. 128, no. 4, pp. 2753-2778, Feb. 2023. https://doi.org/10.1109/ACCESS.2025.3543127.

[4] J. M. Vidal, M. A. S. Monge and S. M. M. Monterrubio, "Anomaly-based intrusion detection: Adapting to present and forthcoming communication environments" *in Handbook of Research on Machine and Deep Learning Applications for Cyber Security, Hershey,* PA, USA:IGI Global, pp. 195-218, 2020. doi: 10.4018/978-1-5225-9611-0.ch010.

[5] L.Wang, et al., "Research on Alarm Reduction of Intrusion Detection System Based on Clustering and Whale Optimization Algorithm", *Appl.Sci.,* 2021. https://doi.org/10.3390/app112311200.

[6] X.Hoanng, et al., "Future internet botnet detection based on the ML techniques using DNS Query Data", *Future Internet,* 2018. https://doi.org/10.3390/fi10050043.

[7] R.Khan, et al., "An Adaptive Multi-Layer Botnet Det.Tech.Using ML Classifiers", *Appl.Sc.,* 2019. https://doi.org/10.3390/app9112375.

[8] J.Kim, et al., "The impact of imbalanced training data on ML for author name disombiguation", *Scientometrics,* 2018. https://doi.org/10.1109/CISCT57197.2023.10351278.

[9] R, G. et al. (2021). "Simulation Process of Injection Molding and Optimization for Automobile Instrument Parameter in Embedded System" *Advances in Materials Science and Engineering,* vol. 2021, Article ID 9720297, 10 pages, 2021. https://doi.org/10.1155/2021/9720297.

[10] Y.B.Zikria, et al., "Deep learning for intelligent IoT: Opportunities challenges and solutions", Computer Communications, 2020. https://doi.org/10.1016/j.comcom.2020.08.017

[11] A.Kim, et al., "AI-IDS: Application of deep learning to real-time Web intrusion detection", *IEEE Access,* 2020. https://doi.org/10.1109/ACCESS.2020.2986882.

[12] H.Alqahtani, et al., "Cyber intrusion detection using machine learning classification techniques", COMS2, 2020. https://doi.org/10.1007/978-981-15-6648-6_10.

[13] X.Liu, et al., "Malicious data injection attacks risk mitigation strategy of cyber-physical power system based on hybrid measurements attack detection and risk propagation", IJEPES, 2022. https://doi.org/10.1016/j.ijepes.2022.108241.

[14] J.Tian, et al., "Datadriven false data injection attacks against cyber-physical power systems", *Computers & Security,* 2022. https://doi.org/10.1016/j.cose.2022.102836.

[15] M.Dehghani, et al., "Fourier singular values-based false data injection attack detection in AC smart-grids", *Applied Sciences,* 2021. https://doi.org/10.3390/app11125706.

[16] J. Verma, A. Bhandari and G. Singh, "Review of existing data sets for network intrusion detection system", *Advances in Mathematics: Scientific Journal,* vol. 9, no. 6, pp. 3849-3854, 2020. https://doi.org/10.37418/amsj.9.6.

[17] G. R. et al. (2021). "An Unconventional Approach for Analyzing the Mechanical Properties of Natural Fiber Composite Using Convolutional Neural Network" *Advances in Materials Science and Engineering,* vol. 2021, Article ID 5450935, 15 pages, 2021. https://doi.org/10.1155/2021/5450935.

[18] E. U. H. Qazi, M. H. Faheem and T. Zia, "HDLNIDS: Hybrid Deep-Learning-Based Network Intrusion Detection System", *Applied Sciences,* vol. 13, no. 8, pp. 4921, 2023. https://doi.org/10.3390/app13084921.

[19] N. Koroniotis, N. Moustafa, E. Sitnikova and B. Turnbull, "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset", *Future Generation Computer Systems,* vol. 100, pp. 779-796, 2019. https://doi.org/10.1016/j.future.2019.05.041.

[20] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, M. Ghogho and F. El Moussa, "Deepids: Deep learning approach for intrusion detection in software defined networking", *Electronics,* vol. 9, no. 9, pp. 1533, 2020. https://doi.org/10.3390/electronics9091533.

[21] I. Martins, J. S. Resende, P. R. Sousa, S. Silva, L. Antunes and J. Gama, "Host-based IDS: A review and open issues of an anomaly detection system in IoT", *Future Gener. Comput. Syst.,* vol. 133, pp. 95-113, Aug. 2022. https://doi.org/10.1016/j.future.2022.03.001.

[22] K. He, D. D. Kim and M. R. Asghar, "Adversarial machine learning for network intrusion detection systems: A comprehensive survey", *IEEE Commun. Surveys Tuts.,* vol. 25, no. 1, pp. 538-566, 1st Quart. 2023. https://doi.org/10.1109/COMST.2022.3233793.

[23] S.Jain, et al., "Data mining Classification Techniques for Intrusion Detection System", CICN-20, 2020.

https://doi.org/10.1109/CICN49253.2020.9242642.

[24] S.K.Sahu, et al., *"Botnet Detection in Network Traffic Based on GBM"*, IJESC, 2021.

[25] Y.Wang, et al., "Intell.Alarm Drop for Distributed Intrusion Det.Sys.via EC", ACISP, 2019. https://doi.org/10.1109/CISCT57197.2023.10351278.

[26] P. K. Donta, S.N. Srirama, T. Amgoth and C. S. R. Annavarapu, "Survey on recent advances in IoT application layer protocols and machine learning scope for research directions", *Digit. Commun. Netw.*, vol. 8, no. 5, pp. 727-744, 2022. https://doi.org/10.1016/j.dcan.2021.10.004.

[27] T.J.N, et al Machine learning models to detect the blackhole attack in wireless adhoc network, Materials Today: Proceedings, Vol. 47, Part 1, 2021, pp.235-239, ISSN: 2214-7853, https://doi.org/10.1016/j.matpr.2021.04.129.

[28] S. Liang et al., "YOLO Edge: Real-time intelligent object detection system based on edge-cloud cooperation in autonomous vehicles", *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 12, pp. 25345-25360, Dec. 2022. https://doi.org/10.1109/TITS.2022.3158253.

[29] Z. Li, J. Song, K. Qiao, C. Li, Y. Zhang and Z. Li, "Research on efficient feature extraction: Improving YOLOv5 backbone for facial expression detection in live streaming scenes", *Front. Comput. Neurosci*, vol. 16, 2022. doi: 10.1109/ACCESS.2018.2877890.

[30] Information Security Classification Framework (QGISCF), Feb. 2024, [Online]. https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/information-security-classification-framework-qgiscf (Accessed Date: November 10, 2024).

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare.